REMARKS

Favorable reconsideration of this application is respectfully requested.

The specification is amended by the present response to delete the noted hyperlinks as suggested in the Office Action.

Claims 1-24 are pending in this application. Claims 1-24 were rejected under 35 U.S.C. § 103(a) as unpatentable over "Bluetooth Specification", Bluetooth Security, November 29, 1999, pages 149-178 (herein "Bluetooth") in view of "5C Digital Transmission Content Protection White Paper" Revision 1.0, July 14, 1998, pages 1-13 (herein "5C White Paper").

Addressing the above-noted rejection, that rejection is traversed by the present response.

Applicants respectfully submit the claims as currently written distinguish over the applied art as the claims recite specific operations of how first and second encryption keys are utilized to transmit copy protected contents data securely, and such specific combined usage of the first and second encryption keys is not taught or suggested by the combination of teachings in the Bluetooth reference and the 5C White Paper.

One objective of the present invention is to provide enhanced transfer of copyright protected contents data, and to particularly realize a secure copyright protection even in a radio network environment.[1]

With reference to Fig. 1 in the present specification as a non-limiting example, the present invention can be applied to a radio communication system including a portable MPEG4 player 101 and a portable viewer 102, which are both owned by the same person and thus that are authorized to communicate information with each other. The portable MPEG4 player 101 and the portable viewer 102 are located within an area in which a connection by a

[1] See for example the present specification at page 3, lines 3-6.

local area radio network is possible. Further, another portable viewer 103 owned by a different entity may also enter that local area, but the claimed system prevents that other portable viewer 103 from viewing data from the portable MPEG4 player 101 as the other portable viewer 103 is owned by a different entity and does not have authorization to view data provided from the portable MPEG4 player 101.

The outstanding rejection is not fully considering the claimed features, and particularly that in the claimed invention the second authentication unit carries out its second authentication using the first encryption key from the first encryption operation.

In further detail, the outstanding rejection relies on the Bluetooth reference to disclose each of the claimed "first authentication unit" and "first key exchange unit". The outstanding Office Action recognizes that the Bluetooth reference does not disclose the claimed "second authentication unit" and the claimed "second key exchange unit". To cure those recognized deficiencies in the Bluetooth reference the outstanding rejection cites the 5C White Paper to disclose copy protection system through authentication, exchange key, and encrypting contents data being exchanged.

The outstanding rejection is further based on the position that:

> . . . it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the authentication and key exchange taught by Bluetooth to establish a secure communication link between authorized devices with 5C White Paper's teaching of providing copy protection system for protecting contents data through a second authentication and key exchanged by encrypting the content data with the content key to ensure the copyrighted content data is securely managed.[2]

Applicants submit the basis for the outstanding rejection is not fully considering that in the claimed invention the second authentication is carried out ***after*** the first authentication and by ***using the first encryption key from the first authentication***. That is, the claims recite

[2] The basis for the outstanding rejection is noted in the Office Action of June 7, 2006 at pages 5-6.

a specific operation in which a first authentication is utilized to judge whether or not a receiving device is a device that is allowed to communicate with the transmitting device or for enabling the receiving device to operate as a device that is allowed to communicate with the transmitting device. As shown for example in Figure 5 in the present specification at steps S1-S19, a first authentication is carried out to determine whether two devices can properly communicate with each other, such as devices 101 and 102 in Figure 1 in the present specification (steps S1-S16). When it is determined that those two devices can communicate with each other a first encryption key is shared between the two devices (steps S18-S19). That shared first encryption key is then utilized in a second authentication operation (in steps S21-S23).

Thereby, in the claimed invention the second authentication unit carries out a second authentication with the receiving device for protecting copyright of the contents data to be transmitted through an encrypted radio communication using the first authentication key.

With such a claimed structure, even if a receiving device in the claimed invention does not have a copyright protection function, the receiving device can communicate with a transmitting device because the second authentication is carried out after the first authentication is carried out. If the second authentication was carried out before the first authentication was carried out the receiving device would not be able to communicate with a transmitting device.

Neither the Bluetooth reference nor the 5C White Paper teach or suggest a first authentication and a second authentication being carried out in the specific order noted above. In the claimed invention since the second authentication is carried out after the first authentication is carried out a receiving device even without a copyright protection function can communicate with a transmitting device. The Bluetooth reference and the 5C White Paper do not even allude to realizing such a result.

Stated another way, the Bluetooth reference and the 5C White Paper disclose two different authentication systems that are similar to each other in that they perform authentication through a key exchange and encrypting. What the present invention realizes is combining two different systems in a specific order so that a first authentication process can be utilized to determine whether two devices can properly communicate with each other, and then a second authentication process is utilized using results from the first authentication process. Neither the Bluetooth reference nor the 5C White Paper teach or suggest combining such features.

In that respect applicants note the Bluetooth reference and the 5C White Paper themselves do not teach or suggest being combined in any manner. Each of those references discloses individual authentication through key exchange processes, and there is no disclosure in either reference for the suggested combination.

Moreover, applicants note the claimed invention also requires a specific order of combining two separate authentication and key exchange processes. There is clearly no teaching or suggestion in the Bluetooth reference and the 5C White Paper to be combined in a specific order to meet the claimed limitation. That is, there is absolutely no teaching or suggestion in the Bluetooth reference or the 5C White Paper that would suggest that one of ordinary skill in the art to utilize the authentication and key exchang in the Bluetooth reference initially, and then additionally utilize the authentication and key exchange in the 5C White Paper using results from that first authentication. It is only the applicants of the present invention that have recognized the benefits that can be realized in the claimed invention by combining two different authentication and key exchange operations. No reference has been cited to teach such a combination.

A further more specific detailed example of the operation in the present invention attention is now explained with reference to Figure 5 in the present specification.

The claimed invention utilizes a specific sequence of communication between the MPEG4 player 101 and the portable viewer 102 to assure secure communication and to ensure that the portable viewer 103 cannot view data from the portable MPEG4 player 101. As discussed in the present specification at page 20, line 1 to page 21, line 31 and with respect to Fig. 5 in the present specification, such a sequence of communicating between the MPEG4 player 101 and the portable viewer 102 is carried out as follows:

(1) a Bluetooth layer link key sharing procedure is carried out (step S13) when PIN code values on both devices coincide;

(2) a value of a link key K1 to be used in a subsequent authentication and key exchange is shared (steps S14 and S15);

(3) a Bluetooth layer authentication procedure and a Bluetooth layer key exchange procedure are carried out (steps S16 and S17);

(4) a value of a Bluetooth first encryption key (layer encryption key Kbt) is shared (steps S18 and S19);

(5) a DTCP authentication and key exchange are carried out by utilizing a Bluetooth layer level encryption (step S20);

(6) a value of a second encryption key (second encryption key Kc) is shared on a DTCP layer (copyright protection layer) (steps S21 and S22);

(7) the portable MPEG4 player 101 transmits contents (MPEG4 data) to be transmitted by encrypting them by using the second encryption key Kc, to the portable viewer 102 (steps S23 and S24); and

(8) the portable viewer 102 decrypts the received encrypted contents by using the DTCP level second encryption key Kc (step S25).

Another transferring sequence between the portable MPEG4 player 101 and the portable viewer 102 can be carried out according to the following processes (as noted in the present specification at page 25 lines 7-25 and Fig. 9);

(1) the portable MPEG4 player 101 encrypts the contents (MPEG4 data) to be transmitted by using the encryption key first, and then encrypts the copyright protected contents by using the encryption key Kbt (step S54); and

(2) the portable viewer 102 decrypts the received encrypted contents by using the encryption key Kbt first, and then the decrypted contents by using the encryption key Kc (step S54).

Thus, according to the present invention, it is possible to share the encryption key properly only between the legitimate devices that can successfully complete the authentication procedure, so that it becomes possible to realize the data transfer using the cipher communication only between devices that have properly shared the encryption key.

In contrast to the specific operation in the claimed invention, the Bluetooth reference and the 5C White Paper both are only broadly directed to copy protection system through authentication, key exchange, and an encrypting contents data. Neither reference teaches or suggests how two different copy protection operations and encryption keys can be utilized in the order claimed to effectively transmit copyright protected contents data securely and simply.

Applicants also draw attention to claims 6, 15, 20, and 23-24 which allow setting up an encrypted communication path encrypting using the second encryption key on the encrypted radio communication which is encrypted by using the first encryption key. Such features are believed to also clearly distinguish over the Bluetooth reference in view of the 5C White Paper.

In view of the foregoing comments the claims as currently written are believed to clearly distinguish over the applied Bluetooth reference in view of the 5C White Paper.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 06/04)

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

EHK:SNS\dt
I:\ATTY\SNS\21's\213200\213200US-AF.DOC